Journal of Combinatorial Theory, Series A 117 (2010) 827–841

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Schur rings over a Galois ring of odd characteristic

Sergei Evdokimov [1], Ilya Ponomarenko [2]

Steklov Institute of Mathematics, St. Petersburg, Russian Federation

ARTICLE INFO

Article history:
Received 29 December 2008
Available online 24 December 2009

Keywords:
Schur ring
Galois ring
Normal cyclotomic ring
Generalized wreath product

ABSTRACT

It is proved that any Schur ring over a Galois ring of odd characteristic is either normal, or of rank 2, or a non-trivial generalized wreath product. The normal Schur rings are characterized as a special subclass of the cyclotomic Schur rings.

1. Introduction

In papers [11,12] K.H. Leung and S.H. Man proved that any Schur ring (S-ring) over a finite cyclic group can be constructed from special S-rings by means of two operations: tensor product and wedge product (as for a background of S-rings see Section 7). This theorem supplemented with the normality theory from [5] enabled to get a series of strong results in algebraic combinatorics [5,6,10,14].

To generalize the Leung–Man theorem in some way to S-rings over an arbitrary abelian group, the notion of an S-ring over a commutative ring R [3] was introduced in [7]; by definition any such ring is an S-ring over the additive group R^+ of the ring R that is invariant with respect to its multiplicative group $R^\times$. It should be noted that by the Schur theorem on multipliers any S-ring over a cyclic group of order n can be treated as an S-ring over the ring $R = \mathbb{Z}_n$ of integers modulo n. We observe that in this case R is the direct product of Galois rings of coprime characteristics with prime residue fields. Thus it is natural to generalize the Leung–Man theorem to S-rings over the products of arbitrary Galois rings of coprime characteristics. In the present paper (which is the first step in the indicated direction) we do this when R is a Galois ring of odd characteristic with the special rings being S-rings of rank 2 and pure cyclotomic S-rings defined in Section 2. Only one operation is needed here: it is the generalized wreath product also defined in that section.

E-mail addresses: evdokim@pdmi.ras.ru (S. Evdokimov), inp@pdmi.ras.ru (I. Ponomarenko).

[1] The work was partially supported by RFFI Grants 07-01-00485 and 06-01-00471.
[2] The work was partially supported by RFFI Grants 07-01-00485, 08-01-00379 and 08-01-00640.

[3] All rings are supposed to be finite rings with identity.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2009.12.008

Theorem 1.1. *Any S-ring over a Galois ring of odd characteristic is either pure cyclotomic, or of rank* 2*, or a non-trivial generalized wreath product.*

Theorem 1.1 is an immediate consequence of Theorems 2.11 and 5.1 proved in this paper. Indeed, let $\mathcal{A}$ be a non-rank 2 S-ring over a Galois ring of odd characteristic. If $\mathcal{A}$ is not a non-trivial generalized wreath product, then by Theorem 2.11 the hypothesis of Theorem 5.1 is satisfied. Thus by the latter theorem the ring $\mathcal{A}$ is pure cyclotomic.

As it was said above the Leung–Man theorem was substantially strengthened in [5]. The key point there is the notion of a normal S-ring over a group. The analog of normality for S-rings over a ring is introduced in Section 2.3. It should be noted that the 1–1 correspondence between normal S-rings and normal Cayley schemes over a group that was defined in [5, Section 4.3], induces a 1–1 correspondence between normal (resp. pure) cyclotomic S-rings and normal (resp. corresponding to pure groups) cyclotomic schemes over a ring defined in [8, Section 1].

Let $\mathcal{A}$ be a normal S-ring over a Galois ring of odd characteristic. Then by Corollary 2.14 and Theorem 5.1 we conclude that either $\mathcal{A}$ is pure cyclotomic or $\mathrm{rk}(\mathcal{A}) = 2$. However, in the latter case from Theorem 2.12 and Corollary 2.3 it follows that $\mathcal{A}$ is also cyclotomic. Thus using the characterization of normal cyclotomic schemes over a Galois ring of odd characteristic given in [8] we obtain the following result.

Theorem 1.2. *An S-ring $\mathcal{A}$ over a Galois ring R of odd characteristic is normal if and only if $\mathcal{A}$ is pure cyclotomic, and* $\mathrm{rk}(\mathcal{A}) > 2$ *unless R is a field of order* 3*.*

The following statement is straightforward from Theorems 1.1 and 1.2.

Theorem 1.3. *Any S-ring over a Galois ring of odd characteristic is either normal, or of rank* 2*, or a non-trivial generalized wreath product.*

Concerning finite rings and permutation groups we refer to [13] and [3]. To make the paper self-contained, we cite the background on Schur rings and Galois rings in Sections 7 and 3 respectively. In the latter section we also study multiplicative subgroups in Galois rings. The theory of S-rings over a commutative ring is the subject of Sections 2 and 4. Theorem 6.1 used in Section 4 is proved in Section 6. Finally, Section 5 contains Theorem 5.1 which is a key point for Theorem 1.1.

Notation. As usual by $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ we denote the ring of integers, the ring of rationals and the field of complex numbers respectively.

For a commutative ring R with identity we denote by $R^\times$ and $\mathrm{rad}(R)$ the multiplicative group of R and the radical of R respectively.

The set of all ideals of R is denoted by $\mathcal{I}(R)$. Given $I \in \mathcal{I}(R)$ we denote by I^+ the additive group of I, and by π_I the natural epimorphism from R to R/I.

For a set $X \subset R$ we denote by $I_{\mathrm{U}}(X)$ the smallest ideal of R containing X, and by $I_{\mathrm{L}}(X)$ the largest ideal I of R such that $X + I = X$. Also we set

$$\mathrm{ann}(X) = \{r \in R\colon rX = \{0\}\}$$

and write $\mathrm{ann}(r)$ instead of $\mathrm{ann}(\{r\})$ for $r \in R$.

The group ring of a group G over R is denoted by RG. For $X \subset G$ we set $\xi(X) = \sum_{x\in X} x$.

The group of all permutations of R of the form $x \mapsto ax^\sigma + b$ where $a \in R^\times$, $b \in R$, $\sigma \in \mathrm{Aut}(R)$, is denoted by $\mathrm{A\Gamma L}_1(R)$. The stabilizer of the point 0 in the latter group is denoted by $\Gamma\mathrm{L}_1(R)$.

For a finite local commutative ring R the Teichmüller group and the group of principal units are denoted by $\mathcal{T}$ and $\mathcal{U}$ respectively. Then

$$R^\times = \mathcal{T} \times \mathcal{U},$$

and the groups $\mathcal{T}$ and $\mathcal{U} = 1 + \mathrm{rad}(R)$ are a cyclic group of order $q-1$ and an abelian p-group respectively, where q and p are the order and the characteristic of the residue field $R/\mathrm{rad}(R)$ respectively.

The cardinality of a finite set X is denoted by $|X|$.

2. Schur rings over a commutative ring

2.1. Let R be a finite commutative ring with identity. In this paper we consider the permutation group induced by the action of the group $R^\times$ on the set R by multiplication. It is a subgroup of the group $\mathrm{Aut}(R^+)$, leaves any ideal of R fixed, and has $R^\times$ as a regular faithful orbit.

Let $\mathcal{A}$ be an S-ring over the group R^+. The following definition is taken from [7].

Definition 2.1. We say that $\mathcal{A}$ is an S-ring over the ring R if it is invariant with respect to the action of the group $R^\times$ on $\mathbb{Z}R^+$ by multiplication.

This is equivalent to say that $uX \in \mathcal{S}(\mathcal{A})$ for all $u \in R^\times$ and $X \in \mathcal{S}(\mathcal{A})$. The S-ring of rank 2 and the group ring are obvious examples of S-rings over the ring R. One more example generalizing the latter one is given in the paragraph after the next one.

It should be remarked that there is a lot of S-rings over R^+ that are not S-rings over R. For example, if R is a field, then any S-ring over R is cyclotomic (Corollary 2.3). Therefore the number of all of them is at most $|R^\times|$, whereas the number of S-rings over the group R^+ can be much larger (because R^+ is an elementary abelian group in this case). An explicit example is as follows: let $|R| = p^n$ where p is a prime and $n \geqslant 2$, and H a proper subgroup of $G = R^+$. Then the S-ring over G with the basic sets $\{1_G\}$, $H \setminus \{1_G\}$ and $G \setminus H$ is not an S-ring over the field R because otherwise we should have $|H| - 1 = |G| - |H|$ which is impossible.

Let K be a subgroup of $R^\times$. Then, obviously, K acts faithfully on the group ring $\mathbb{Z}R^+$ and the set of all K-invariant elements of it forms an S-ring over the group R^+. It is called a *cyclotomic* one and is denoted by $\mathrm{Cyc}(K, R)$. The basic sets of this ring are exactly the orbits of K on R and hence

$$\mathrm{Cyc}(K, R) = \mathrm{span}\bigl\{\xi(X)\colon\ X \in \mathrm{Orb}(K, R)\bigr\}.$$

In fact, $\mathrm{Cyc}(K, R)$ is an S-ring over the ring R because the group $R^\times$ permutes the orbits of K. Since the group K acts semiregularly on $R^\times$, the cyclotomic rings are in 1–1 correspondence to the subgroups of $R^\times$.

In the following statement we describe the structure of a basic set of an S-ring over a ring.

Theorem 2.2. *Let $\mathcal{A}$ be an S-ring over a commutative ring R and $X \in \mathcal{S}(\mathcal{A})$. Then there exists a set $X_0 \subset X$ such that $xR^\times \cap yR^\times = \emptyset$ for all distinct $x, y \in X_0$, and*

$$X = \bigcup_{x \in X_0} xK \quad (\textit{disjoint union}) \tag{1}$$

where $K = \{u \in R^\times\colon\ uX = X\}$.

Proof. The set X is obviously K-invariant. So it is the disjoint union of some K-orbits. Take an element in each of them and denote the obtained set by X_0. Then $X_0 \subset X$ and (1) holds. To complete the proof suppose that $xR^\times \cap yR^\times \neq \emptyset$ for some $x, y \in X_0$, $x \neq y$. Then $ux = y$ where $u \in R^\times$. We note that $uX \in \mathcal{S}(\mathcal{A})$ (Definition 2.1). Since $X \cap uX \neq \emptyset$, this implies that $X = uX$. But then $u \in K$, which contradicts the choice of x and y. □

Corollary 2.3. *In the condition of Theorem* 2.2 *suppose in addition that $X \subset R^\times$. Then $X \in \mathrm{Orb}(K, R)$. In particular, any S-ring over a field is a cyclotomic one.*

For an S-ring $\mathcal{A}$ over the ring R set

$$\mathcal{I}(\mathcal{A}) = \bigl\{I \in \mathcal{I}(R)\colon\ I \in \mathcal{S}^*(\mathcal{A})\bigr\}$$

where the set $\mathcal{S}^*(\mathcal{A})$ is defined as in Section 7.1. The elements of $\mathcal{I}(\mathcal{A})$ are called *$\mathcal{A}$-ideals* of R. We say that $\mathcal{A}$ is *R-primitive* if 0 and R are the only $\mathcal{A}$-ideals of R.

Theorem 2.4. *(See [7].) Let R be a commutative ring such that each primary component of it is local. Then any R-primitive S-ring is either of rank 2 or cyclotomic.*[4] *In the latter case, R is a field.*

Corollary 2.5. *Let R be a local commutative ring other than a field. Then any R-primitive S-ring is of rank 2.*

Let R be an arbitrary commutative ring and $I \in \mathcal{I}(\mathcal{A})$. Then the S-ring $\mathcal{A}_{R^+/I^+}$ is an S-ring over the group $(R/I)^+ = R^+/I^+$. Since the ring $\mathcal{A}$ is $R^\times$-invariant, the latter S-ring is $(R/I)^\times$-invariant. Thus it is an S-ring over the quotient ring R/I; we will denote it by $\mathcal{A}_{R/I}$.

2.2. Let $\mathcal{A}$ be an S-ring over a ring R and $X \in \mathcal{S}^*(\mathcal{A})$. It is well known from elementary theory of S-rings over abelian groups, that the smallest group $U_0 \leqslant R^+$ for which $X \subset U_0$, and the largest group $L_0 \leqslant R^+$ for which $L_0 + X = X$, are $\mathcal{A}$-subgroups. By Definition 2.1 this implies that the groups

$$U = \sum_{u \in R^\times} uU_0, \qquad L = \bigcap_{u \in R^\times} uL_0$$

belong to the set $\mathcal{H}(\mathcal{A})$. Clearly, $U \leqslant I_{\mathrm{U}}(X)$, $L \geqslant I_{\mathrm{L}}(X)$ and $R^\times U = U$, $R^\times L = L$. On the other hand, suppose that the ring R is generated by the units. Then any $R^\times$-invariant subgroup of R^+ is an ideal of R. Thus in this case $I_{\mathrm{U}}(X) = U$ and $I_{\mathrm{L}}(X) = L$, and hence $I_{\mathrm{U}}(X)$ and $I_{\mathrm{L}}(X)$ are $\mathcal{A}$-ideals of R. This proves the following statement.

Theorem 2.6. *Let $\mathcal{A}$ be an S-ring over a commutative ring R. Suppose that R is generated by the units. Then $I_{\mathrm{U}}(X), I_{\mathrm{L}}(X) \in \mathcal{I}(\mathcal{A})$ for all $X \in \mathcal{S}^*(\mathcal{A})$.*

Corollary 2.7. *Let $\mathcal{A}$ be an S-ring over a local commutative ring. Then $I_{\mathrm{U}}(X), I_{\mathrm{L}}(X) \in \mathcal{I}(\mathcal{A})$ for all $X \in \mathcal{S}^*(\mathcal{A})$.*

Proof. Follows from Theorem 2.6 because each element of the radical of a local commutative ring is the difference of two units. □

It is easily seen that given $X \subset R$ we have

$$I_{\mathrm{L}}(X) = I_{\mathrm{L}}(uX) \quad \text{for all } u \in R^\times. \tag{2}$$

Therefore from Definition 2.1 it follows that the ideal $I_{\mathrm{L}}(X)$ does not depend on the set $X \in \mathcal{S}(\mathcal{A})$ such that $X \cap R^\times \neq \emptyset$. We denote this ideal by $I_{\mathrm{L}}(\mathcal{A})$.

Theorem 2.8. *Let $\mathcal{A}$ be an S-ring over a local commutative ring R. Then $I_{\mathrm{L}}(\mathcal{A}) \neq 0$ if and only if there exist proper ideals I, $J \in \mathcal{I}(\mathcal{A})$ such that*

$$J \subset I_{\mathrm{L}}(X) \cap I \quad \text{for each } X \in \mathcal{S}(\mathcal{A}) \text{ with } X \subset R \setminus I. \tag{3}$$

Proof. The sufficiency immediately follows from the definitions. To prove the necessity suppose that $I_{\mathrm{L}}(\mathcal{A}) \neq 0$. Set $J = I_{\mathrm{L}}(\mathcal{A})$ and I a maximal element in the set $\{I' \in \mathcal{I}(\mathcal{A}):\ J \subset I' \neq R\}$. Clearly, $J \subset I$. Take $X \in \mathcal{S}(\mathcal{A})$ such that $X \subset R \setminus I$. Then $X \cap R^\times \neq \emptyset$, for otherwise the ideal generated by X and I is contained in $\mathrm{rad}(R)$ and belongs to $\mathcal{I}(\mathcal{A})$ (Corollary 2.7), which contradicts the maximality of I. So $I_{\mathrm{L}}(X) = J$ by the definition of $I_{\mathrm{L}}(\mathcal{A})$. Thus (3) holds. Since $J = I_{\mathrm{L}}(\mathcal{A}) \neq 0$ and $I \neq R$, we are done. □

If (3) holds for some ideals $I, J \in \mathcal{I}(\mathcal{A})$, we say that $\mathcal{A}$ is a *generalized wreath product* or that $\mathcal{A}$ satisfies *the I/J-condition*. Clearly, it is true whenever $I = R$ or $J = 0$. Theorem 2.8 shows that $I_{\mathrm{L}}(\mathcal{A}) \neq 0$ if and only if the S-ring $\mathcal{A}$ is a non-trivial generalized wreath product in the sense of the following definition, the second part of which is a special case of [5, Definition 5.2].

[4] In the conditions of the theorem "R-primitivity" is equivalent to "quasiprimitivity" in sense of [7] (see the remark before Theorem 1.3 of that paper).

Definition 2.9. We say that $\mathcal{A}$ is a non-trivial generalized wreath product if there exist proper ideals $I, J \in \mathcal{I}(\mathcal{A})$ such that (3) holds. In this case we also say that $\mathcal{A}$ satisfies the I/J-condition non-trivially.

It should be noted that in the sense of [4] the S-ring $\mathcal{A}$ satisfying the I/J-condition is the (standard) generalized wreath product of the S-rings $\mathcal{A}_I$ and $\mathcal{A}_{R/J}$ over the groups I^+ and $(R/J)^+$ respectively. Moreover, the latter S-ring can be treated as an S-ring over the ring R/J whereas the former one when I is a principal ideal can be treated as an S-ring over the ring $R/\operatorname{ann}(I)$.

2.3. Following [8] a non-empty set $X \subset R$ is called *pure* if $I_{\mathrm{L}}(X) = 0$. This means that the only ideal I for which $X + I = X$ is the zero one. Due to (2) the sets X and uX are pure or not simultaneously. Therefore any subset of a pure orbit of a subgroup of $R^\times$ is also pure. It should be noted that if X is such a pure orbit, the set $\pi_I(X)$ where I is an ideal of R, is not necessarily pure. However, if $I = I_{\mathrm{L}}(X)$, the set $\pi_I(X)$ is pure for all $X \subset R$.

Definition 2.10. The S-ring $\mathcal{A}$ is called *pure* if $I_{\mathrm{L}}(\mathcal{A}) = 0$.

It follows that $\mathcal{A}$ is pure if and only if some (and hence any) $X \in \mathcal{S}(\mathcal{A})$ such that $X \cap R^\times \neq \emptyset$ is pure. The S-rings of rank 2 are obvious examples of pure S-rings. If $K \leqslant R^\times$ is a pure group (i.e. pure as a subset of R), then the cyclotomic ring $\mathrm{Cyc}(K, R)$ is also pure. Non-pure S-rings over a local ring can be characterized by means of Theorem 2.8 as follows.

Theorem 2.11. *An S-ring over a local commutative ring is not pure if and only if it is a non-trivial generalized wreath product.*

We say that an S-ring $\mathcal{A}$ over a commutative ring R is *normal* if

$$\operatorname{Aut}(\mathcal{A}) \leqslant \Gamma\mathrm{L}_1(R) \tag{4}$$

where the group $\operatorname{Aut}(\mathcal{A})$ is defined as in Section 7.1. Suppose that $\operatorname{rk}(\mathcal{A}) = 2$. Then obviously $T \operatorname{Aut}(\mathcal{A}) = \operatorname{Sym}(R)$ where T is the group of all translations of R; in particular, the group $T \operatorname{Aut}(\mathcal{A})$ is primitive. On the other hand, if the ring R is local, then $\operatorname{rad}(R)$ is a block of the group $\mathrm{A}\Gamma\mathrm{L}_1(R) \leqslant \operatorname{Sym}(R)$. Since any block of a primitive group is trivial, we come to the following statement.

Theorem 2.12. *Let $\mathcal{A}$ be a normal S-ring over a local commutative ring R. If $\operatorname{rk}(\mathcal{A}) = 2$, then R is a field.*

The following statement provides a necessity condition for a cyclotomic S-ring over a Galois ring to be normal (cf. [8, Theorem 1.4]).

Theorem 2.13. *Let $\mathcal{A}$ be a normal S-ring over a local commutative ring R with the residue field of order q. Suppose that $\mathcal{A}$ satisfies the I/J-condition non-trivially for some ideals $I, J \in \mathcal{I}(R)$. Then $q = 2$ and $J \subset \operatorname{ann}((2, \operatorname{rad}(R)^2))$.*

Proof. By the theorem hypothesis we have $I \subset \operatorname{rad}(R)$ and $J \neq 0$. The inclusion together with Theorem 7.2 imply that given $a \in J$ the permutation $f_a \in \operatorname{Sym}(R)$ defined by

$$x^{f_a} = \begin{cases} x + a, & \text{if } x \in \mathcal{U}, \\ x, & \text{otherwise}, \end{cases}$$

belongs to $\operatorname{Aut}(\mathcal{A})$ where $\mathcal{U}$ is the group of principal units of R. On the other hand, from the normality of $\mathcal{A}$ it follows that $x^{f_a} = bx^\sigma$ for some $b \in R^\times$ and $\sigma \in \operatorname{Aut}(R)$, and all $x \in R$. Since $1^{f_a} = a + 1$, we conclude that $b = a + 1$. Thus,

$$x^\sigma = x/(1 + a), \quad x \in R \setminus \mathcal{U}. \tag{5}$$

This implies that σ leaves fixed each set $x + \mathrm{rad}(R)$. Since $\mathcal{T}^\sigma = \mathcal{T}$ and $|\mathcal{T} \cap (x + \mathrm{rad}(R))| = 1$ for $x \in R^\times$ where $\mathcal{T}$ is the Teichmüller group of R, we see that σ leaves fixed each element of $\mathcal{T}$. Therefore $t = t^\sigma = t/(1+a)$ for all $t \in \mathcal{T} \setminus \{1\}$. If $q > 2$, then the latter set is not empty whence it follows that $a = 0$. Thus in this case $J = 0$. Contradiction. This proves that $q = 2$. But then $2 \in \mathrm{rad}(R)$, and hence due to (5) we have $2 = 2/(1+a)$. So $2a = 0$ and $J \subset \mathrm{ann}(2)$. On the other hand, given $x, y \in \mathrm{rad}(R)$ we have

$$xy/(1+a) = (xy)^\sigma = x^\sigma y^\sigma = xy/(1+a)^2,$$

whence it follows that $axy = 0$. Therefore $J \subset \mathrm{ann}(\mathrm{rad}(R)^2)$. □

Corollary 2.14. *Any normal S-ring over a Galois ring of odd characteristic is pure.*

Proof. Follows from Theorems 2.13 and 2.11. □

3. Multiplicative subgroups in Galois rings

3.1. Following [13, Section XVI] a local ring R is called *Galois* if it is a Galois extension of the prime ring $\mathbb{Z}_{p^n}$ for some prime p and positive integer n, or equivalently if $\mathrm{rad}(R) = pR$. Given positive integers n, d there exists a unique (up to isomorphism) Galois ring of characteristic p^n with the residue field of order $q = p^d$; it is denoted by $\mathrm{GR}(p^n, d)$. We observe that

$$\mathrm{GR}(p, d) \cong \mathrm{GF}\big(p^d\big), \qquad \mathrm{GR}\big(p^n, 1\big) \cong \mathbb{Z}_{p^n}.$$

Each ideal of the Galois ring $\mathrm{GR}(p^n, d) = R$ other than R is of the form $p^i R$, $i = 1, \ldots, n$, and the corresponding quotient ring is isomorphic to $\mathrm{GR}(p^i, d)$. It is known that R^+ is a homocyclic p-group of rank d and exponent p^n, i.e. it is isomorphic to a direct product of d cyclic p-groups of order p^n. If p is odd, then the group $\mathcal{U} = 1 + pR$ is homocyclic of rank d and exponent p^{n-1}; the set of its elements of order dividing p^{n-i} equals $\mathcal{U}_i = 1 + p^i R$, $i = 1, \ldots, n$.

In this subsection we deduce several consequences from the following statement proved in [8, Theorem 6.6].

Lemma 3.1. *Let R be a Galois ring of odd characteristic, $K \leqslant R^\times$ a group and $I \in \mathcal{I}(R)$. Then the group $\pi_I(K)$[5] is pure whenever so is K.*

The following general lemma will be used in proving Theorem 3.3 below.

Lemma 3.2. *Let R be a commutative ring. Then given $r \in R$ and $X \subset R$ we have*

$$r\pi^{-1}\big(I_{\mathrm{L}}\big(\pi(X)\big)\big) = I_{\mathrm{L}}(rX)$$

where $\pi = \pi_I$ with $I = \mathrm{ann}(r)$.

Proof. Denote by f the R-module endomorphism $x \mapsto rx$ of R. Then $\ker(f) = \mathrm{ann}(r)$ and $\mathrm{im}(f) = rR$. Therefore f induces an R-module isomorphism $g : R/I \to rR$. Clearly, g induces a bijection from the set $\{J \in \mathcal{I}(R)\colon\ J \supset I\}$ onto the set $\{J \in \mathcal{I}(R)\colon\ J \subset rR\}$. So

$$g\big(I_{\mathrm{L}}(Y)\big) = I_{\mathrm{L}}\big(g(Y)\big), \quad Y \subset R/I. \tag{6}$$

(Here $I_{\mathrm{L}}(Y) \in \mathcal{I}(R/I)$ and $I_{\mathrm{L}}(g(Y)) \in \mathcal{I}(R)$, see Notation.) Besides, $\ker(\pi) = \ker(g)$. So $g(Y) = f(\pi^{-1}(Y))$ for all $Y \subset R/I$. Thus from (6) we obtain that

$$r\pi^{-1}\big(I_{\mathrm{L}}\big(\pi(X)\big)\big) = f\big(\pi^{-1}\big(I_{\mathrm{L}}\big(\pi(X)\big)\big)\big) = I_{\mathrm{L}}\big(f(X)\big) = I_{\mathrm{L}}(rX)$$

for all $X \subset R$. □

[5] As for the definition of the epimorphism π_I see Notation.

Below we use a simple observation that any group $K \leqslant R^\times$ naturally acts on each set $p^i R^\times$ where i is a non-negative integer; the corresponding set of K-orbits is denoted by $\mathrm{Orb}(K, p^i R^\times)$.

Theorem 3.3. *Let $R = \mathrm{GR}(p^n, d)$ with p odd, and $K \leqslant R^\times$. Then given $i \in \{0, \dots, n\}$ we have*

(1) $I_{\mathrm{L}}(\pi(K)) = \pi(I_{\mathrm{L}}(K))$ *where* $\pi = \pi_{p^{n-i}R}$,
(2) $I_{\mathrm{L}}(X) = p^i I_{\mathrm{L}}(K)$ *for all* $X \in \mathrm{Orb}(K, p^i R^\times)$.

Proof. Let us prove statement (1). From Lemma 3.1 it follows that this statement is true when the group K is pure. Suppose that $I_{\mathrm{L}}(K) \neq 0$. By induction without loss of generality we can assume that $i = n-1$. However, in this case $I_{\mathrm{L}}(K) \supset p^{n-1}R$ and hence the equality $I_{\mathrm{L}}(\pi(K)) = \pi(I_{\mathrm{L}}(K))$ is obvious. To prove statement (2) let $X = xK$ where $x = p^i u$ with $u \in R^\times$. Then by statement (1) and Lemma 3.2 with $r = x$ and $X = K$ we have

$$\begin{aligned} I_{\mathrm{L}}(X) = I_{\mathrm{L}}(xK) &= x\pi^{-1} I_{\mathrm{L}}\big(\pi(K)\big) = x\pi^{-1}\big(\pi\big(I_{\mathrm{L}}(K)\big)\big) \\ &= xI_{\mathrm{L}}(K) = p^i u I_{\mathrm{L}}(K) = p^i I_{\mathrm{L}}(K). \qquad \square \end{aligned}$$

Corollary 3.4. *Any orbit of a pure multiplicative subgroup in a Galois ring of odd characteristic is pure.*

The following useful statement is one more consequence of Lemma 3.1. It can also be easily deduced from the homocyclicity of the group $\mathcal{U}$ (in the odd characteristic case) by means of the theorem on a basis of a p-group [1, p. 105, Proposition 23.1].

Lemma 3.5. *Let $R = \mathrm{GR}(p^n, d)$ with p odd, $K \leqslant \mathcal{U}$ and $K_i = K \cap \mathcal{U}_i$ where $i = 1, \dots, n$. Then for any $i \in \{1, \dots, n-1\}$ we have $[K_i : K_{i+1}] \leqslant p^d$ with the equality attained if and only if $K_i = \mathcal{U}_i$.*

Proof. Clearly, $[K_i : K_{i+1}] \leqslant [\mathcal{U}_i : \mathcal{U}_{i+1}] = p^d$ for all i. If $K_i = \mathcal{U}_i$ for some i, then $K_{i+1} = \mathcal{U}_{i+1}$ and hence $[K_i : K_{i+1}] = p^d$. Let us prove the converse statement by induction on $n - i$. It is easily seen that if $i = n-1$, then $K_{i+1} = \mathcal{U}_{i+1} = \{1\}$ and hence $|K_i| = p^d = |\mathcal{U}_i|$. Since $K_i \leqslant \mathcal{U}_i$, this shows that $K_i = \mathcal{U}_i$. Suppose that $i < n-1$. Then $K_{i+1} \cap \mathcal{U}_{n-1} = K_i \cap \mathcal{U}_{n-1}$, and hence

$$\begin{aligned} \big[\pi(K_i) : \pi(K_{i+1})\big] &= \big[K_i/(K_i \cap \mathcal{U}_{n-1}) : K_{i+1}/(K_{i+1} \cap \mathcal{U}_{n-1})\big] \\ &= \big[K_i/(K_i \cap \mathcal{U}_{n-1}) : K_{i+1}/(K_i \cap \mathcal{U}_{n-1})\big] = [K_i : K_{i+1}] = p^d \end{aligned}$$

where $\pi = \pi_{p^{n-1}R}$. On the other hand, obviously $\pi(K_i) = \pi(K)_i$ and $\pi(K_{i+1}) = \pi(K)_{i+1}$. Then by the induction hypothesis (applied to the ring $\pi(R) = \mathrm{GR}(p^{n-1}, d)$, the group $\pi(K)$ and i) we have $\pi(K_i) = \pi(\mathcal{U}_i)$. However, $I_{\mathrm{L}}(K_i) \neq 0$, for otherwise $I_{\mathrm{L}}(\pi(K_i)) = 0$ by Lemma 3.1 and then $\pi(\mathcal{U}_i) = \pi(\mathcal{U}_n)$ which is impossible because $i < n-1$. Therefore $\mathcal{U}_{n-1} \leqslant K_i$ and hence $K_i = \pi^{-1}(\pi(K_i)) = \pi^{-1}(\pi(\mathcal{U}_i)) = \mathcal{U}_i$. $\square$

3.2. In this subsection basing on the properties of multiplicative subgroups in a Galois ring we prove Theorem 3.7 which will be used in Section 5. We need the following lemma. Below for a ring R, a set $X \subset R$ and an ideal $I \in \mathcal{I}(R)$ we set $X_{I,x} = X \cap (x + I)$ for all $x \in R$.

Lemma 3.6. *Let $R = \mathrm{GR}(p^n, d)$ with p odd, K a subgroup of $R^\times$ with $I_{\mathrm{L}}(K) = p^{n-l}R$ where $l \geqslant 1$, and $J = p^m R$ an ideal of R with $m \leqslant n$. Suppose that for some $y \in p^{l-1}R^\times$, $z \in p^l R^\times$ we have*

$$|Y_{J,y}| = |Z_{J,z}|$$

where $Y = yK$, $Z = zK$. Then $m = n$ whenever $l \leqslant m-1$.

Proof. Suppose that $l \leqslant m-1$. Let $x \in X \in \mathrm{Orb}(K, p^j R^\times)$ where $0 \leqslant j \leqslant l$. Then

$$X_{J,x} = X \cap (x + J) = x(K \cap \mathcal{U}_{m-j}) = xK_{m-j}$$

where for any $i = 1, \ldots, n$ we set $K_i = K \cap \mathcal{U}_i$. Besides, $\mathcal{U}_{n-j} \leqslant \mathcal{U}_{m-j}$ because $m \leqslant n$, and $\mathcal{U}_{n-j} \leqslant K$ because $j \leqslant l$. Therefore, $K_{m-j} \geqslant \mathcal{U}_{n-j}$. Since the point stabilizer $(R^\times)_x$ of x in $R^\times$ equals $\mathcal{U}_{n-j}$, it follows that $(K_{m-j})_x = \mathcal{U}_{n-j}$ and hence $|(K_{m-j})_x| = |p^{n-j}R| = p^{jd}$. Thus,

$$|X_{J,x}| = \big[K_{m-j} : (K_{m-j})_x\big] = |K_{m-j}|/p^{jd}.$$

By the lemma hypothesis this implies that

$$|K_{m-l+1}|/p^{(l-1)d} = |Y_{J,y}| = |Z_{J,z}| = |K_{m-l}|/p^{ld}$$

whence $[K_{m-l} : K_{m-l+1}] = p^d$. By Lemma 3.5 we have $K_{m-l} = \mathcal{U}_{m-l}$, and hence $\mathcal{U}_{m-l} \leqslant K$. Therefore $p^{n-l}R \geqslant I_{\mathrm{L}}(K) \geqslant p^{m-l}R$. Since $m \leqslant n$, it follows that $m = n$. □

Theorem 3.7. *Let $\mathcal{A}$ be a pure S-ring over a Galois ring R of odd characteristic p^n. If $\mathrm{rk}(\mathcal{A}) > 2$, then $\mathrm{rad}(R)$ is an $\mathcal{A}$-ideal of R.*

Proof. Take $X \in \mathcal{S}(\mathcal{A})$ such that $X \cap R^\times \neq \emptyset$, and set

$$J = \max\big\{I \in \mathcal{I}(\mathcal{A}):\ X \subset R \setminus I\big\}.$$

It suffices to show that $J = \mathrm{rad}(R)$. Suppose that this is not true. Then $J = p^m R$ where $2 \leqslant m \leqslant n$. First, we observe that the set $X_i = X \cap p^i R^\times$ is non-empty for $i = 0, \ldots, m-1$, or equivalently that $\mathrm{tr}(X) = R \setminus J$ where

$$\mathrm{tr}(X) = \bigcup_{u \in R^\times} uX.$$

Indeed, $\mathrm{tr}(X)$ is an $\mathcal{A}$-subset of R such that $R^\times \subset \mathrm{tr}(X) \subset R \setminus J$. Therefore, if $\mathrm{tr}(X) \neq R \setminus J$, then one can find a set $Y \in \mathcal{S}(\mathcal{A})$ such that $Y \subset \mathrm{rad}(R) \setminus J$. This implies that $J \subsetneq I_{\mathrm{U}}(Y) \subset \mathrm{rad}(R)$ which contradicts the definition of J by Corollary 2.7. Thus all the X_i's are non-empty and

$$\big|(X_i)_{J,y}\big| = |X_{J,y}| = |X_{J,z}| = \big|(X_j)_{J,z}\big|, \quad y \in X_i,\ z \in X_j,\ i, j = 0, \ldots, m-1 \tag{7}$$

(see equality (20)).

Next, set $K = \{u \in R^\times:\ uX = X\}$. Then by Theorem 2.2 we have

$$X_i \in \mathrm{Orb}\big(K, p^i R^\times\big), \quad i = 0, \ldots, m-1. \tag{8}$$

Let us define a non-negative integer l by the condition $I_{\mathrm{L}}(K) = p^{n-l}R$. Since $m \geqslant 2$, there exists $x \in X \cap \mathrm{rad}(R)$. Then obviously $(1 + I_0)\{x\} = \{x\}$ where $I_0 = p^{n-1}R$. This implies that $(1 + I_0)X = X$ and hence $1 + I_0 \leqslant K$. Therefore $I_0 \subset I_{\mathrm{L}}(K)$ whence it follows that $l \geqslant 1$. On the other hand, due to (8) from statement (2) of Theorem 3.3 it follows that

$$I_{\mathrm{L}}(X_i) = p^{n-l+i}R, \quad i = 0, \ldots, m-1. \tag{9}$$

Thus, $l \leqslant m-1$, for otherwise $I_0 \subset I_{\mathrm{L}}(X)$ which contradicts the purity of X. Therefore due to (7) the hypothesis of Lemma 3.6 is satisfied for all $y \in X_{l-1}$ and $z \in X_l$. So by this lemma $m = n$ and hence $J = 0$. Next, from the definition of J it follows that the S-ring $\mathcal{A}$ is R-primitive. So by Corollary 2.5 we have $\mathrm{rk}(\mathcal{A}) = 2$. Contradiction. Thus $J = \mathrm{rad}(R)$. □

4. Duality

4.1. Let R be a Galois ring of characteristic p^n and $\hat{R} = \hat{R}^+$ the group dual to the group R^+ (see Section 7.2). Clearly,

$$\bigl(p^i R\bigr)^{\perp} = p^{n-i}\hat{R}, \quad i = 0, \ldots, n. \tag{10}$$

Take $\chi \in \hat{R}$ so that the image of χ contains a primitive p^nth root of unity. Then

$$\hat{R} = \bigl\{\chi^{(r)}\colon r \in R\bigr\}$$

where $\chi^{(r)}$ is the character of R^+ such that $\chi^{(r)}(x) = \chi(rx)$, $x \in R$ (see e.g. [9]). It follows that the additively written group $\hat{R}$ together with the multiplication defined by the formula

$$\chi^{(r)}\chi^{(s)} = \chi^{(rs)}, \quad r, s \in R,$$

becomes a ring. Its zero and identity elements are the principal character of R^+ and the character χ respectively. We say that $\hat{R}$ is the ring *dual* to R (with respect to χ). It is a Galois ring isomorphic to R: the isomorphism is given by $r \mapsto \chi^{(r)}$. Clearly,

$$\hat{R}^{\times} = \bigl\{\chi^{(r)}\colon r \in R^{\times}\bigr\}, \qquad \operatorname{rad}(\hat{R}) = \bigl\{\chi^{(r)}\colon r \in pR\bigr\}. \tag{11}$$

The image of a group $K \leqslant R^{\times}$ with respect to the above isomorphism is denoted by $\hat{K}$.[6]

Theorem 4.1. *Let R be a Galois ring of characteristic p^n and $S \neq \emptyset$ a pure subset of R. Then*

(1) *given $S' \subset R \setminus S$ there exists $\chi \in \hat{R}^{\times}$ such that $\chi(S) \neq \chi(S')$,*
(2) *given $\chi \in \hat{R}^{\times}$ there exists $r \in R^{\times}$ such that $\chi(rS) \neq 0$.*

Proof. To prove statement (1) suppose on the contrary that $\chi(S) = \chi(S')$ for all $\chi \in \hat{R}^{\times}$. However, when χ runs over $\hat{R}^{\times}$ its extension $\psi : \mathbb{Q}G \to \mathbb{C}$ where $G = R^+$, runs over the set $\Psi = \Psi_{\mathbb{Q}}(G)$ defined in Theorem 6.1. Thus $\xi(S) - \xi(S') \in \ker(\psi)$ for all $\psi \in \Psi$. Since the group G is homocyclic, by Theorem 6.1 this implies that $\xi(S) - \xi(S') \in (\xi(I))$ where I is the minimal ideal of the ring R. Since $S \cap S' = \emptyset$, the set S is a union of additive I-cosets. Therefore S is not pure, which contradicts the hypothesis of the theorem. To prove statement (2) let $\chi \in \hat{R}^{\times}$. By statement (1) with $S' = \emptyset$ there exists a character $\chi' \in \hat{R}^{\times}$ such that $\chi'(S) \neq \chi'(S') = 0$. However, due to (11) we have $\chi' = \chi^{(r)}$ for some $r \in R^{\times}$. Thus, $\chi(rS) = \chi'(S) \neq 0$. □

4.2. Let $\mathcal{A}$ be an S-ring over a Galois ring R, $\hat{R}$ the ring dual to R with respect to a character χ and $\hat{\mathcal{A}}$ the S-ring over the group $\hat{R}^+$ that is dual to $\mathcal{A}$ (see Section 7.2).

Theorem 4.2. *The ring $\hat{\mathcal{A}}$ is an S-ring over the ring $\hat{R}$.*

Proof. Suppose that $\chi^{(s)}$ and $\chi^{(t)}$ belong to the same basic set of $\hat{\mathcal{A}}$ where $s, t \in R$. Then given $r \in R^{\times}$ we have $\chi^{(s)}(rS) = \chi^{(t)}(rS)$, or equivalently

$$\chi^{(rs)}(S) = \chi^{(rt)}(S), \quad S \in \mathcal{S}(\mathcal{A}).$$

Since $\chi^{(rs)} = \chi^{(r)}\chi^{(s)}$ and $\chi^{(rt)} = \chi^{(r)}\chi^{(t)}$, this implies that the characters $\chi^{(r)}\chi^{(s)}$ and $\chi^{(r)}\chi^{(t)}$ belong to the same basic set of $\hat{\mathcal{A}}$ for all $r \in R^{\times}$. Thus the required statement follows from (11). □

[6] Since the set $\hat{R}^{\times} = \hat{R} \setminus p\hat{R}$ does not depend on the character χ, any S-ring over the ring dual to R with respect to χ is also an S-ring over the ring dual to R with respect to any other character belonging to $\hat{R}^{\times}$.

We observe that if $\mathrm{char}(R) = p^n$ then $\mathcal{I}(R) = \{p^i R\colon\ i = 0, \dots, n\}$ and $\mathcal{I}(\hat{R}) = \{p^i \hat{R}\colon\ i = 0, \dots, n\}$. Therefore by (10) and (22) we have

$$\mathcal{I}(\hat{\mathcal{A}}) = \bigl\{I^{\perp}\colon\ I \in \mathcal{I}(\mathcal{A})\bigr\}. \tag{12}$$

Thus $\mathcal{A}$ is R-primitive if and only if $\hat{\mathcal{A}}$ is $\hat{R}$-primitive (as for the R-primitivity see Section 2.1). Moreover, from (12) and Theorem 7.3 we obtain the following statement.

Theorem 4.3. *Let $\mathcal{A}$ be an S-ring over a Galois ring. Then the ring $\mathcal{A}$ is a non-trivial generalized wreath product if and only if so is the ring $\hat{\mathcal{A}}$. More exactly, $\mathcal{A}$ satisfies the I/J-condition if and only if $\hat{\mathcal{A}}$ satisfies the $J^{\perp}/I^{\perp}$-condition.*

Corollary 4.4. *Let $\mathcal{A}$ be an S-ring over a Galois ring. Then $\mathcal{A}$ is pure if and only if so is $\hat{\mathcal{A}}$.*

Proof. Follows from Theorems 4.3 and 2.11. □

The following theorem shows that an S-ring and its dual are cyclotomic or not simultaneously. This can be also deduced from the results of [9] by using the well-known 1–1 correspondence between S-rings and translation association schemes.

Theorem 4.5. *Let $\mathcal{A} = \mathrm{Cyc}(K, R)$ where $K \leqslant R^{\times}$. Then $\hat{\mathcal{A}} = \mathrm{Cyc}(\hat{K}, \hat{R})$.*

Proof. Let $X \in \mathrm{Orb}(\hat{K}, \hat{R})$. Then given $\chi_1, \chi_2 \in X$ there exists $r \in K$ such that $\chi_1 = \chi_2^{(r)}$. Since $S = rS$ for each basic set S of $\mathcal{A}$, this implies that

$$\chi_1(S) = \chi_2^{(r)}(S) = \chi_2(rS) = \chi_2(S), \quad S \in \mathcal{S}(\mathcal{A}).$$

So $\mathcal{A}' \geqslant \hat{\mathcal{A}}$ where $\mathcal{A}' = \mathrm{Cyc}(\hat{K}, \hat{R})$. On the other hand, $\mathrm{rk}(\hat{\mathcal{A}}) = \mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\mathcal{A}')$. Thus $\hat{\mathcal{A}} = \mathcal{A}'$. □

5. Pure S-rings over a Galois ring

In this section we prove the following theorem.

Theorem 5.1. *Let $\mathcal{A}$ be an S-ring over a Galois ring R of odd characteristic. Suppose that $\mathcal{A}$ is pure and $\mathrm{rk}(\mathcal{A}) \geqslant 3$. Then $\mathcal{A}$ is pure cyclotomic.*

Proof. We need two lemmas.

Lemma 5.2. *In the conditions of Theorem* 5.1 *we have $\mathcal{I}(\mathcal{A}) = \mathcal{I}(R)$.*

Proof. Let $\mathrm{char}(R) = p^n$ and $I = pR$, $J = p^{n-1}R$. By Corollary 4.4 the S-ring $\hat{\mathcal{A}}$ over the Galois ring $\hat{R}$ is pure. So from Theorem 3.7 it follows that $p\hat{R}$ is an $\hat{\mathcal{A}}$-ideal. By formulas (10) and (12) this implies that $J \in \mathcal{I}(\mathcal{A})$. On the other hand, from Theorem 3.7 it follows that $I \in \mathcal{I}(\mathcal{A})$. Therefore $\mathcal{I}(\mathcal{A}) = \mathcal{I}(R)$ for $n \leqslant 2$. If $n \geqslant 3$, then $\mathrm{rk}(\mathcal{A}_{R/J}) > 2$ because $\pi_J(I)$ is a proper $\mathcal{A}_{R/J}$-ideal. Thus by induction we conclude that $\mathcal{I}(\mathcal{A}_{R/J}) = \mathcal{I}(R/J)$. Since J is the minimal ideal of R, it follows that $\mathcal{I}(\mathcal{A}) = \mathcal{I}(R)$. □

Lemma 5.3. *Let $\mathcal{A}$ be an S-ring over a Galois ring R and $K \leqslant R^{\times}$. Suppose that $\mathcal{I}(\hat{\mathcal{A}}) = \mathcal{I}(\hat{R})$ and $\mathrm{Orb}(K, R^{\times}) \subset \mathcal{S}^*(\mathcal{A})$. Then any pure orbit of the group $\hat{K}$ in $\hat{R}$ belongs to $\mathcal{S}^*(\hat{\mathcal{A}})$.*

Proof. Let X_1 be a pure orbit of the group $\hat{K}$. Then $X_1 = \chi_1^{\hat{K}}$ for some character $\chi_1 \in \hat{R}$. Denote by X the basic set of $\hat{\mathcal{A}}$ containing χ_1 and set $X_2 = \chi_2^{\hat{K}}$ where $\chi_2 \in X$. Since $\mathcal{I}(\hat{\mathcal{A}}) = \mathcal{I}(\hat{R})$, the set $Y = \hat{R}^{\times}\chi_1$ belongs to $\mathcal{S}^*(\hat{\mathcal{A}})$. This implies that $X \subset Y$ whence it follows that $\chi_1, \chi_2 \in Y$, and hence $X_1, X_2 \subset Y$.

Denote by a the cardinality of the kernel of the natural action of the group K on the set Y. Since the action is semiregular, given $S \in \mathrm{Orb}(K, R^\times)$ and $s \in S$ we have

$$\chi_i(S) = \sum_{r\in K} \chi_i(rs) = \sum_{r\in K} \chi_i^{(r)}(s) = as(X_i), \quad i = 1, 2,$$

where $s(X_i)$ is defined by (21) with $G = \hat{R}^+$, $S = X_i$ and χ being the character of G corresponding to s. On the other hand, as $S \in \mathcal{S}^*(\mathcal{A})$ the definition of the dual S-ring implies that $\chi_1(S) = \chi_2(S)$. Thus $s(X_1) = s(X_2)$ for all $s \in R^\times$. Now due to the purity of the set X_1, from statement (1) of Theorem 4.1 applied to $\hat{R}$ and X_1, X_2 it follows that $X_1 = X_2$ and hence $\chi_2 \in X_1$. However, χ_2 is an arbitrary element of X. Thus $X \subset X_1$ and we are done. □

From Lemma 5.2 it follows that

$$\mathcal{I}(\mathcal{A}) = \mathcal{I}(R). \tag{13}$$

By Corollary 2.3 this implies that the basic set of $\mathcal{A}$ containing 1_R, say K, is a subgroup of $R^\times$ and

$$\mathrm{Orb}\big(K, R^\times\big) \subset \mathcal{S}(\mathcal{A}). \tag{14}$$

Moreover, due to (12) and (13) we have $\mathcal{I}(\hat{\mathcal{A}}) = \mathcal{I}(\hat{R})$. So by Lemma 5.3 any pure orbit of the group $\hat{K}$ belongs to $\mathcal{S}^*(\hat{\mathcal{A}})$. However, since the S-ring $\mathcal{A}$ is pure, the group K and hence the group $\hat{K}$ are also pure. So by Corollary 3.4 all orbits of $\hat{K}$ are pure. Thus $\hat{\mathcal{A}} \geqslant \mathrm{Cyc}(\hat{K}, \hat{R})$, and consequently by Theorem 4.5

$$\mathcal{A} \geqslant \mathrm{Cyc}(K, R).$$

This shows that any orbit of K is a union of basic sets of $\mathcal{A}$. Therefore to prove that $\mathcal{A} = \mathrm{Cyc}(K, R)$ it suffices to verify that these basic sets are equal.

Suppose on the contrary that S_1 and S_2 are distinct basic sets contained in an orbit of the group K. We observe that since the orbit is pure, these sets are also pure (see the beginning of Section 2.3). Therefore, by Theorem 4.1 (with $S = S_1$ and $S' = S_2$ for statement (1), and with $S = K$ for statement (2)) there exist a character $\chi \in \hat{R}$ and a set $T \in \mathrm{Orb}(K, R^\times)$ such that

$$\chi(S_1) \neq \chi(S_2), \qquad \chi(T) \neq 0. \tag{15}$$

On the other hand, due to the supposition and (14) we have $S_1, S_2 \subset \mathrm{rad}(R)$. Since $\xi(S_1), \xi(T) \in \mathcal{A}$ and $T \subset R^\times$, this implies that the product $\xi(S_1)\xi(T)$ belongs to the subset $\mathcal{A} \cap \mathrm{span}(R^\times)$ of the ring $\mathbb{Z}R^+$, and hence it is K-invariant. Taking into account that $S_2 = rS_1$ for some $r \in K$, we conclude that

$$\xi(S_1)\xi(T) = \xi(rS_1)\xi(rT) = \xi(S_2)\xi(T).$$

Applying χ to both sides of this equality we obtain a contradiction with (15). □

6. A theorem on characters

The following statement on representations of a homocyclic p-group is a generalization of [11, Proposition 2.7].

Theorem 6.1. *Let G be a homocyclic finite group of exponent p^n, $n \geqslant 1$, and let $K \subset \mathbb{C}$ be a field linearly separated from $\mathbb{Q}[w]$ over $\mathbb{Q}$ where w is a primitive p^nth root of unity. Denote by $\Psi = \Psi_K(G)$ the set of all K-epimorphisms $\psi : KG \to K[w]$. Then*

$$\bigcap_{\psi\in\Psi} \ker(\psi) = I_K(G_0) \tag{16}$$

where $G_0 = G^{p^{n-1}}$ and $I_K(G_0)$ is the ideal of KG generated by $\xi(G_0)$.

Proof. It is easily seen that the restriction of any homomorphism $\psi \in \Psi$ to the group G_0 is a non-principal irreducible character of this group. So $\psi(\xi(S)) = 0$ for all $S \in G/G_0$. Since $I_K(G_0)$ is the linear span of the elements $\xi(S)$, this implies that $I_K(G_0) \subset \ker(\psi)$. Thus $I_K(G_0)$ is a subset of the left-hand side of (16).

To prove the converse inclusion we need two auxiliary lemmas. Below given $f, g \in G$ we set

$$\alpha_f(g) = \left|\left\{\psi \in \Psi\colon\ f^{-1}g \in H_\psi\right\}\right|$$

where $H_\psi = \{g \in G\colon\ \psi(g) = 1\}$.

Lemma 6.2. *If $gG_0 = g'G_0$, then $\alpha_f(g) = \alpha_f(g')$ for all $f \in G \setminus \{g, g'\}$.*

Proof. Due to the homocyclicity of G the group $\mathrm{Aut}(G)$ acts transitively on the elements of the same order. Since obviously $(H_\psi)^\sigma = H_{\psi^\sigma}$ for all $\sigma \in \mathrm{Aut}(G)$ where ψ^σ is the element of Ψ taking ξ to $\psi(\xi^\sigma)$, we conclude that

$$o\bigl(f^{-1}g\bigr) = o\bigl(\bigl(f'\bigr)^{-1}g'\bigr) \quad \Rightarrow \quad \alpha_f(g) = \alpha_{f'}\bigl(g'\bigr)$$

for all $f, f' \in G$ where $o(x)$ denotes the order of $x \in G$. This proves the required statement because $o(f^{-1}g) = o(f^{-1}g')$ unless $f \in \{g, g'\}$. (Indeed, if $o(f^{-1}g) > p$, then obviously $o(f^{-1}g) = o(f^{-1}g')$, whereas otherwise $o(f^{-1}g) \neq o(f^{-1}g')$ only if $f = g$ or $f = g'$.) □

Let $\xi = \sum_{g\in G} a_g g$ be an element of KG. Denote by C the group of all p^nth roots of unity in $\mathbb{C}$. For $c \in C$ and $\psi \in \Psi$ set

$$A_c = \sum_{g \in G \cap \psi^{-1}(c)} a_g.$$

Lemma 6.3. *Suppose that $\xi \in \ker(\psi)$. Then for each $S \in G/G_0$ the number $A_{\psi(g)}$ does not depend on $g \in S$.*

Proof. Denote by $\psi_0 : KC \to K[w]$ the epimorphism identical on the group C. Since the restriction of ψ to G induces an epimorphism from G to C, there exists a unique epimorphism $\varphi : KG \to KC$ such that $\psi = \varphi \circ \psi_0$. By the lemma hypothesis this implies that $\varphi(\xi) \in \ker(\psi_0)$. Therefore taking into account that $G \cap \varphi^{-1}(c) = G \cap \psi^{-1}(c)$ for all $c \in C$, we conclude that the right-hand side of the obvious formula

$$\varphi(\xi) = \sum_{g\in G} a_g \varphi(g) = \sum_{c\in C}\Biggl(\sum_{g\in G\cap\varphi^{-1}(c)} a_g\Biggr)c = \sum_{c\in C} A_c c$$

also belongs to $\ker(\psi_0)$. On the other hand, from [11, Proposition 2.7] it follows that

$$\ker(\psi_0) = I_K(C_0) = \mathrm{span}_K\bigl\{\xi(T)\colon\ T \in C/C_0\bigr\} \tag{17}$$

where C_0 is the group of pth roots of unity. Thus for each C_0-coset of C the number A_c does not depend on the choice of c in this coset (we used that $\psi(G_0) = C_0$). The lemma is proved. □

To complete the proof of the theorem suppose that ξ belongs to the left-hand side of (16). To prove that $\xi \in I_K(G_0)$ it suffices to verify that given $S \in G/G_0$ the number a_g does not depend on $g \in S$. First, we observe that given $g \in G$ we have

$$\sum_{\psi\in\Psi} A_{\psi(g)} = \sum_{\psi\in\Psi}\sum_{h\in gH_\psi} a_{gh} = \sum_{f\in G}\alpha_f(g)a_f.$$

If $g' \in gG_0$, then from Lemma 6.3 it follows that $A_{\psi(g)} = A_{\psi(g')}$ and hence

$$\sum_{f\in G}\alpha_f(g)a_f = \sum_{f\in G}\alpha_f\bigl(g'\bigr)a_f. \tag{18}$$

By Lemma 6.2 this implies that

$$\alpha_g(g)a_g + \alpha_{g'}(g)a_{g'} = \alpha_g(g')a_g + \alpha_{g'}(g')a_{g'}.$$

Since obviously $\alpha_g(g) = |\Psi| = \alpha_{g'}(g')$ and $\alpha_{g'}(g) = \alpha_g(g')$, we conclude that

$$\bigl(|\Psi| - \alpha_g(g')\bigr)(a_g - a_{g'}) = 0. \tag{19}$$

However, when ψ runs over Ψ the group H_ψ runs over the set of all maximal homocyclic subgroups of G of exponent p^n. Therefore $\bigcap_{\psi\in\Psi} H_\psi = \{1\}$, and hence $\alpha_g(g') < |\Psi|$ whenever $g \neq g'$. By (19) this shows that $a_g = a_{g'}$ and we are done. □

7. S-rings over a finite group

7.1. Let G be a finite group. A subring $\mathcal{A}$ of the group ring $\mathbb{Z}G$ is called a *Schur ring* (*S-ring*, for short) over G if it has a (uniquely determined) $\mathbb{Z}$-basis consisting of the elements $\xi(X) = \sum_{x\in X} x$ where X runs over a family $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of pairwise disjoint non-empty subsets of G such that

$$\{1\} \in \mathcal{S}, \quad \bigcup_{X\in\mathcal{S}} X = G \quad \text{and} \quad X \in \mathcal{S} \quad \Rightarrow \quad X^{-1} \in \mathcal{S}.$$

We call the elements of $\mathcal{S}$ the *basic* sets of $\mathcal{A}$ and denote by $\mathcal{S}^*(\mathcal{A})$ the set of all unions of them and by $\mathcal{H}(\mathcal{A})$ the set of all subgroups of G in $\mathcal{S}^*(\mathcal{A})$. The elements of $\mathcal{S}^*(\mathcal{A})$ and $\mathcal{H}(\mathcal{A})$ are called *$\mathcal{A}$-subsets of G* (or *$\mathcal{A}$-sets*) and *$\mathcal{A}$-subgroups of G* respectively. The number

$$\mathrm{rk}(\mathcal{A}) = \dim_{\mathbb{Z}}(\mathcal{A})$$

is called the *rank* of $\mathcal{A}$.

Let $H \leqslant G$ and $X \subset G$. Then X is a disjoint union of the sets

$$X_{H,x} = X \cap Hx$$

where x runs over a right transversal of G by H. On the other hand, obviously $\xi(H)\xi(X_{H,x}) = |X_{H,x}|\xi(Hx)$. Thus if $H \in \mathcal{H}(\mathcal{A})$ and $X \in \mathcal{S}(\mathcal{A})$, then

$$|X_{H,x}| = |X_{H,y}|, \quad x, y \in X \tag{20}$$

(the coefficient of $\xi(X)\xi(H)$ in $\xi(X)$ coincides with $|X_{H,x}|$ for all $x \in X$).

Let $H \in \mathcal{H}(\mathcal{A})$. Then $\{X \in \mathcal{S}\colon\ X \subset H\}$ is the set of basic sets of an S-ring over the group H. This S-ring is denoted by $\mathcal{A}_H$. If the group H is normal and $\pi : G \to G/H$ is the quotient epimorphism, then $\{\pi(X)\colon\ X \in \mathcal{S}\}$ is the set of basic sets of an S-ring over the group G/H. This S-ring is denoted by $\mathcal{A}_{G/H}$.

Definition 7.1. Let $\mathcal{A}$ be an S-ring over a group G and let L, U be subgroups of G. We say that $\mathcal{A}$ satisfies the *U/L-condition* if the following three conditions hold:

(1) $L \leqslant U$ and L is normal in G,
(2) $L, U \in \mathcal{H}(\mathcal{A})$,
(3) $LX = XL = X$ for all $X \in \mathcal{S}(\mathcal{A})$ with $X \subset G \setminus U$.

If, moreover, $L \neq \{1\}$ and $U \neq G$, we say that $\mathcal{A}$ satisfies the U/L-condition non-trivially.

An S-ring $\mathcal{A}$ satisfying the U/L-condition was called in [11,12] the wedge product of the S-rings $\mathcal{A}_U$ and $\mathcal{A}_{G/L}$. It should be noted that the authors in [4] independently introduced the external operation of the generalized wreath product of two S-rings which produces exactly the S-rings satisfying the U/L-condition.

The following statement shows that any S-ring $\mathcal{A}$ over G that satisfies the U/L-condition non-trivially contains special non-trivial automorphisms. By definition a permutation $f \in \mathrm{Sym}(G)$ is an automorphism of $\mathcal{A}$ if $1^f = 1$ and the elements xy^{-1} and $x^f(y^f)^{-1}$ belong to the same basic set of $\mathcal{A}$ for all $x, y \in G$. Below the group of all automorphisms of $\mathcal{A}$ is denoted by $\mathrm{Aut}(\mathcal{A})$.

Theorem 7.2. *Let $\mathcal{A}$ be an S-ring over a group G that satisfies the U/L-condition. Then given a mapping $t : G/U \to L$ with $t(U) = 1$, the permutation $x \mapsto x\,t(Ux)$ of G belongs to* $\mathrm{Aut}(\mathcal{A})$.

Proof. Follows from [5, Lemma 5.6] for $f_1 = \mathrm{id}_U$ and $f_2 = \mathrm{id}_{G/L}$. □

7.2. Let $\mathcal{A}$ be an S-ring over a finite abelian group G and $\hat{G}$ the group dual to G, i.e. the group of all irreducible $\mathbb{C}$-characters of G. Given $S \subset G$ and $\chi \in \hat{G}$ set

$$\chi(S) = \sum_{s \in S} \chi(s). \tag{21}$$

Characters $\chi_1, \chi_2 \in \hat{G}$ are called equivalent if $\chi_1(S) = \chi_2(S)$ for all $S \in \mathcal{S}(\mathcal{A})$. Denote by $\hat{\mathcal{S}}$ the set of classes of this equivalence relation. Then the submodule of $\mathbb{Z}\hat{G}$ spanned by the elements $\xi(X)$, $X \in \hat{\mathcal{S}}$, is an S-ring over $\hat{G}$ (see [2, Theorem 6.3]). This ring is called *dual* to $\mathcal{A}$ and is denoted by $\hat{\mathcal{A}}$. Obviously, $\mathcal{S}(\hat{\mathcal{A}}) = \hat{\mathcal{S}}$. Moreover, $\mathrm{rk}(\hat{\mathcal{A}}) = \mathrm{rk}(\mathcal{A})$ and

$$\mathcal{H}(\hat{\mathcal{A}}) = \left\{H^\perp\colon\ H \in \mathcal{H}(\mathcal{A})\right\} \tag{22}$$

where $H^\perp = \{\chi \in \hat{G}\colon\ H \leqslant \ker(\chi)\}$. It is also true that the S-ring dual to $\hat{\mathcal{A}}$ is equal to $\mathcal{A}$.

Theorem 7.3. *Let $\mathcal{A}$ be an S-ring over an abelian group G. Then the ring $\mathcal{A}$ is a non-trivial generalized wreath product if and only if so is the ring $\hat{\mathcal{A}}$. More exactly, $\mathcal{A}$ satisfies the U/L-condition if and only if $\hat{\mathcal{A}}$ satisfies the $L^\perp/U^\perp$-condition.*

Proof. Since $(1_G)^\perp = \hat{G}$ and $G^\perp = 1_{\hat{G}}$, it suffices to verify only the second part of the theorem. To do this suppose that $\mathcal{A}$ satisfies the U/L-condition for some $U, L \in \mathcal{H}(\mathcal{A})$. Then $U^\perp, L^\perp \in \mathcal{H}(\hat{\mathcal{A}})$ and $U^\perp \leqslant L^\perp$. Therefore to verify that the S-ring $\hat{\mathcal{A}}$ satisfies the $L^\perp/U^\perp$-condition it suffices to prove that given a basic set $\hat{X} \subset \hat{G} \setminus L^\perp$ of $\hat{\mathcal{A}}$ we have $\hat{X}\psi = \hat{X}$ for all characters $\psi \in U^\perp$. By the definition of the dual S-ring all we need to verify is that given $\chi \in \hat{X}$ and $\psi \in U^\perp$ we have

$$\chi(S) = \chi\psi(S), \quad S \in \mathcal{S}(\mathcal{A}). \tag{23}$$

Let us consider two cases. If $S \subset U$, then by the choice of ψ we have $\psi(x) = 1$ for all $x \in S$. Therefore $\chi(S) = \chi\psi(S)$. Now, suppose that $S \subset G \setminus U$. Since the ring $\mathcal{A}$ satisfies the U/L-condition, it follows that the set S is a union of cosets by the group L. On the other hand, since $\chi \in \hat{X} \subset \hat{G} \setminus L^\perp$, we see that $\ker(\chi) \not\subset L$. Besides, since $\ker(\psi) \geqslant U \geqslant L$, we also have $\ker(\chi\psi) \not\subset L$. However, it is well known that $\chi'(L) = 0$, and hence $\chi'(xL) = 0$ where $x \in G$, for any character $\chi' \in \hat{G}$ such that $\ker(\chi') \not\subset L$. Thus $\chi(S) = 0 = \chi\psi(S)$. This proves equality (23). The converse statement follows from the direct one and the equalities $(L^\perp)^\perp = L$ and $(U^\perp)^\perp = U$. □

References

[1] M. Aschbacher, Finite Group Theory, Cambridge Stud. Adv. Math., vol. 10, Cambridge University Press, Cambridge, 1986.
[2] E. Bannai, T. Ito, Algebraic Combinatorics, I, Benjamin/Cummings, Menlo Park, CA, 1984.
[3] J.D. Dixon, B. Mortimer, Permutation Groups, Grad. Texts in Math., vol. 163, Springer-Verlag, New York, 1996.
[4] S. Evdokimov, I. Ponomarenko, On a family of Schur rings over a finite cyclic group, Algebra i Analiz 13 (3) (2001) 139–154; English translation in St. Petersburg Math. J. 13 (3) (2002) 441–451.
[5] S. Evdokimov, I. Ponomarenko, Characterization of cyclotomic schemes and normal Schur rings over a cyclic group, Algebra i Analiz 14 (2) (2002) 11–55; English translation in St. Petersburg Math. J. 14 (2) (2003) 189–221.
[6] S. Evdokimov, I. Ponomarenko, Recognizing and isomorphism testing circulant graphs in polynomial time, Algebra i Analiz 15 (6) (2003) 1–34; English translation in St. Petersburg Math. J. 15 (6) (2004) 813–835.

[7] S. Evdokimov, I. Ponomarenko, A new look at the Burnside–Schur theorem, Bull. Lond. Math. Soc. 37 (2005) 535–546.
[8] S. Evdokimov, I. Ponomarenko, Normal cyclotomic schemes over a finite commutative ring, Algebra i Analiz 19 (2007) 58–84; English translation in St. Petersburg Math. J. 19 (2008) 911–929.
[9] R.W. Goldbach, H.L. Claasen, Cyclotomic schemes over finite rings, Indag. Math. (N.S.) 3 (1992) 301–312.
[10] I. Kovács, Classifying arc-transitive circulants, J. Algebraic Combin. 20 (2004) 353–358.
[11] K.H. Leung, S.H. Man, On Schur rings over cyclic groups, II, J. Algebra 183 (1996) 273–285.
[12] K.H. Leung, S.H. Man, On Schur rings over cyclic groups, Israel J. Math. 106 (1998) 251–267.
[13] B.R. McDonald, Finite Rings with Identity, Pure Appl. Math., vol. 28, Marcel Dekker Inc., New York, 1974.
[14] M. Muzychuk, A solution of the isomorphism problem for circulant graphs, Proc. London Math. Soc. 88 (2004) 1–41.